1.6 二つの平方数の和

ワークシート

問題

STEP II 2023、問 7

先に進む前に、まず問題を読んでおこう。問題は、OCR が配布している 2023 年の STEP 過去問一式（zip ファイル）のうち、STEP II の問題用紙にある：

www.ocr.org.uk/Images/707102-2023-past-papers.zip

ヒント

まずは自力で問題に取り組んでみよう。行き詰まったら、ヒントを**一つずつ**読み、そのたびに問題に戻ること。**手を止めて、やってみよう**と記したヒントが重要な段階である。各ヒントの後には計算用の余白がある。

考えてみよう　a と b を整数として $z = a + ib$ とするとき、$|z|^2$ は何か。

段階 1　絶対値は掛け算と両立する

扱う内容：小問 (i)

手を止めて、やってみよう　zw を展開し、$|zw|^2$ を書き下して展開せよ。得られた式は因数分解（factorise）できるだろうか。

段階 2 それを使う

扱う内容：小問 (ii)

考えてみよう 5 と 221 をそれぞれ二つの平方数の和（sum of two squares）として表せ。$|z|^2 = 5$ や $|w|^2 = 221$ を満たす複素数（complex number）はどのようなものか。

手を止めて、やってみよう 小問 (i) より $|zw|^2 = 5 \times 221$ である。zw を展開すると、その実部（real part）と虚部（imaginary part）が h と k になる。二つ目の答えを得るには、一方の因数の共役（conjugate）を試してみよ。

段階 3　まず因数分解する

扱う内容：小問 (iii) と (iv)

考えてみよう　8045 の末尾は 5 である。因数分解せよ。

手を止めて、やってみよう　もう一方の因数は、ある平方数（perfect square）よりわずかに大きい。どれだけ大きいか、そしてその差は平方数か。そのあとは小問 (ii) と同様に掛け合わせよ。

手を止めて、やってみよう　小問 (iv)：36 はすでに平方数である。絶対値（modulus）の 2 乗が 36 になる複素数はどれか。また、それを掛けると何が起こるか。

段階 4 三通りの表し方

扱う内容：小問 (v)

考えてみよう 小問 (iii) と同様に、大きい方の数はある平方数に近い。まずそれを二つの平方数の和として表せ。

手を止めて、やってみよう 25 は $|\alpha|^2$ の形に二通り以上の方法で表せる。5 はその一つである。$|\alpha|^2 = 25$ を満たすガウス整数（Gaussian integer）はいくつあるか。そのうち、本当に異なる組を与えるのはどれか。

段階 5　割り算

扱う内容：小問 (vi)

考えてみよう　1002037 と 109 を二つの平方数の和として表せ。ここでも近くの平方数を探すとよい。

手を止めて、やってみよう　小問 (ii) から (v) では掛け算をした。この小問ではその考え方を逆向きにたどる。すなわち、一方のガウス整数を他方で割るのである。割り切れない場合は、共役を試してみよ。

背後にある数学

フェルマーの二平方定理

どのような素数が 2 つの平方数の和になるだろうか。$2 = 1^2 + 1^2$、5、13、17、29、37、41 はそうであり、3、7、11、19、23、31 はそうではない。規則はこうである。2 を除けば、素数が 2 つの平方数の和になるのは、それを 4 で割った余りが 1 であるとき、かつそのときに限る。フェルマー（Fermat）は 1640 年にこれを述べ、オイラー（Euler）が 1749 年に証明した。ガウス整数の言葉でいえば、これは次のことを意味

する。素数 $p \equiv 1 \pmod 4$ は $p = (a+bi)(a-bi)$ と**分解する**（split）が、素数 $p \equiv 3 \pmod 4$ は素数のままである。たとえば $5 = (2+i)(2-i)$ であるが、3 はまったく因数分解できない。

1990 年、ドン・ザギエ（Don Zagier）は二平方定理の証明を発表した。それはたった 1 文の長さであることで有名である。この証明は解説つきで *Proofs from THE BOOK* に収められている。

独自の素数をもつ新しい数の体系

ガウス（Gauss）は、ガウス整数が通常の整数と驚くほどよく似た振る舞いをすることに気づいた。除法の原理（division algorithm）とユークリッドの互除法（Euclidean algorithm）があり、すべてのガウス整数はガウス素数（Gaussian prime）の積に（± 1 や $\pm i$ を掛ける違いを除いて）**一意的に**分解される。これを $(\star)$ と組み合わせると、ある数が 2 つの平方数の和として何通りに表せるかを、その素因数分解（prime factorisation）だけから正確に数えることができる。

大学では、これは**代数的整数論**（algebraic number theory）への入り口となる。代数的整数論とは、通常の整数を理解するために $\mathbb{Z}[i]$ や $\mathbb{Z}[\sqrt{-5}]$ のような数の体系を研究する分野である。Section 1.7 では、この分野がなぜ生み出される必要があったのかを示す。このような体系のすべてがガウス整数ほど行儀がよいわけではないのである。

四平方とその先

すべての正の整数は **4 つの**平方数の和である（ラグランジュ（Lagrange）、1770 年）。その証明は $(\star)$ の四平方版に基づいており、それは $(\star)$ が複素数から得られるのと同じようにして、ハミルトン（Hamilton）の**四元数**（quaternions）から得られる。これは Section 7.8 で扱う。

次の一歩

1. **障害。** $4k+3$ の形の数は 2 つの平方数の和にならないことを示せ。（4 を法として平方数はどうなるか？）

2. **2 通り。** 65 と 85 をそれぞれ 2 つの平方数の和として 2 通りに表し、その答えをガウス整数を用いて説明せよ。

3. **4 通り。** $1105 = 5 \times 13 \times 17$ である。1105 を 2 つの正の平方数の和として表す 4 通りの異なる方法を求めよ。なぜ 4 通りなのか。

4 **ガウス素数。** やや難 a, b, c, d を整数として $3 = (a + b\mathrm{i})(c + d\mathrm{i})$ ならば、一方の因数の絶対値は 1 であることを示せ。（絶対値の 2 乗をとれ。）これにより、3 がガウス素数であることがわかる。

さらに学ぶために

- **John Stillwell, *Elements of Number Theory***（Springer）。歴史を交えながら、ガウス整数とその先へと積み上げていく。
- **Aigner & Ziegler, *Proofs from THE BOOK***、第 4 章 “Representing numbers as sums of two squares”（数を 2 つの平方数の和として表す）。
- **Joseph Silverman, *A Friendly Introduction to Number Theory***、平方和とガウス整数に関する章。

詳しい解説付きの解答は第 1.6 節にある：

https://beyondstep.keithmcnulty.org/ja/ch01/two-squares.html

毎週 1 問の STEP の問題を丁寧に解き明かす The STEP Up。メールで無料配信中：keithmcnulty.substack.com